



09-01-05

ISV  
A78

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE  
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Serial No. : 09/655,230  
Appellant : Chung Nan Chang  
Filed : September 5, 2000  
Title : SECURE CRYPTOGRAPHIC KEY EX-  
CHANGE AND VERIFIABLE DIGITAL  
SIGNATURE  
TC/A.U. : 2132  
Examiner : Jung W. Kim

Confirmation No. 7762

Docket No. : 2170  
Customer No.: 23320

MAIL STOP APPEAL BRIEF - PATENTS  
Commissioner for Patents  
Post Office Box 1450  
Alexandria, Virginia 22313-1450

Sir:

**APPEAL BRIEF TRANSMITTAL**

Enclosed herewith are three (3) copies of an Appeal Brief for  
this patent application together with a check in the amount of the  
small entity fee for filing a brief in support of an appeal.

///

///

///

///

///

///

///

///

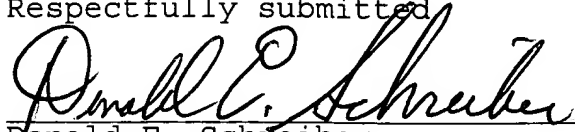
///

///

Appl. No. 09/655,230  
Brief Dated August 29, 2005  
Appeal of

If any additional fee is required, the Commissioner for Patents is hereby authorized to charge any deficiency or credit any surplus in any relevant fee to Deposit Account No. 19-0735. A duplicate copy of this transmittal letter is enclosed herewith.

Respectfully submitted



Donald E. Schreiber  
Reg. No. 29,435

Dated: 29 August, 2005

Donald E. Schreiber  
A Professional Corporation  
Post Office Box 2926  
Kings Beach, CA 96143-2926

Telephone: (530) 546-6041

Attorney for Appellant



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE  
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

EV 550 280 885 US  
"Express Mail" mailing Number

29 August, 2005  
Date of Deposit

I hereby certify that this correspondence is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above addressed to:

MAIL STOP APPEAL BRIEF - PATENTS  
Commissioner for Patents  
Post Office Box 1450  
Alexandria, Virginia 22313-1450

  
Donald E. Schreiber

Dated: 29 August, 2005

Donald E. Schreiber  
A Professional Corporation  
Post Office Box 2926  
Kings Beach, CA 96143-2926  
(530) 546-6041

Serial No. : 09/655,230  
Appellant : Chung Nan Chang  
Filed : September 5, 2000  
Title : SECURE CRYPTOGRAPHIC KEY EX-  
CHANGE AND VERIFIABLE DIGITAL  
SIGNATURE  
TC/A.U. : 2132  
Examiner : Jung W. Kim

Confirmation No. 7762

Docket No. : 2170  
Customer No.: 23320

MAIL STOP APPEAL BRIEF - PATENTS  
Commissioner for Patents  
Post Office Box 1450  
Alexandria, Virginia 22313-1450

Sir:

APPEAL BRIEF

Pursuant to 37 C.F.R. § 1.192, through appellant's undersigned attorney the appellant submits in triplicate the following brief appealing a rejection of claims that appears in an Office Action dated March 29, 2005.

09/02/2005 BABRAHA1 00000047 09655230

01 FC:2402

250.00 OP

Appl. No. 09/655,230  
Brief Dated August 29, 2005  
Appeal of

### **Real Party in Interest**

The real parties in interest are:

1. the inventor, Chung Nan Chang; and
2. an assignee of fifty percent (50%) interest in the patent application, On Line Post Corp. Fl. 12, No. 123, Sec. 2, Chung Hsiao E. Road, 100 Taipei, Taiwan R.O.C.

### **Related Appeals and Interferences**

Appellant is unaware of any presently pending appeal or interference that is related to this appeal.

### **Status of the Claims**

Claims 1-41, set forth in Appendix I hereto, are pending in this application. Claims 1-41 have been finally rejected, and that rejection of claims is being appealed.

### **Status of Amendments**

Claims 1-41 are those originally filed on September 5, 2000.

### **Summary of the Invention**

The invention as embodied in claims 1-41 include four (4) distinct categories of claims.

1. Claims 1-13 encompass a method by which cryptographic units S and R, i.e. sender and receiver, mutually establish a cryptographic key K.
2. Claims 14-26 encompass a system adapted for communicating as an encrypted cyphertext message M a plaintext message P after cryptographic units included in the system establish a cryptographic key K.
3. Claims 27-39 encompass a cryptographic unit adapted for:
  - a. inclusion in a system for communicating as an encrypted cyphertext message M a plaintext message P; and
  - b. establishing a cryptographic key K.
4. Claims 40-41 encompass a method by which a receiving unit R authenticates a sender's digital signature.

For establishing the cryptographic key K, the inventions respectively encompassed by independent claims 1, 14 and 27 all share the following six (6) characteristic elements.

1. A receiving unit R transmits for storage in a publicly accessible repository a plurality of public quantities.<sup>1</sup>

---

<sup>1</sup> Independent claim 1 element a  
Independent claim 14 element c.i.(1)  
Independent claim 27 element a.i.(1)

2. A sending unit S retrieves the plurality of public quantities from the publicly accessible repository.<sup>2</sup>
3. The sending unit S uses at least some of the plurality of public quantities in computing and transmitting to the receiving unit R a plurality of sender's quantities.<sup>3</sup>
4. The receiving unit R uses at least some of the plurality of public quantities and of the plurality of sender's quantities in computing and transmitting to the sending unit S at least one receiver's quantity.<sup>4</sup>
5. The receiving unit R also uses at least some of the plurality of public quantities and of the plurality of sender's quantities in computing the cryptographic key K.<sup>5</sup>

---

<sup>2</sup> Independent claim 1 element b.i.  
Independent claim 14 element c.ii.  
Independent claim 27 element a.ii.

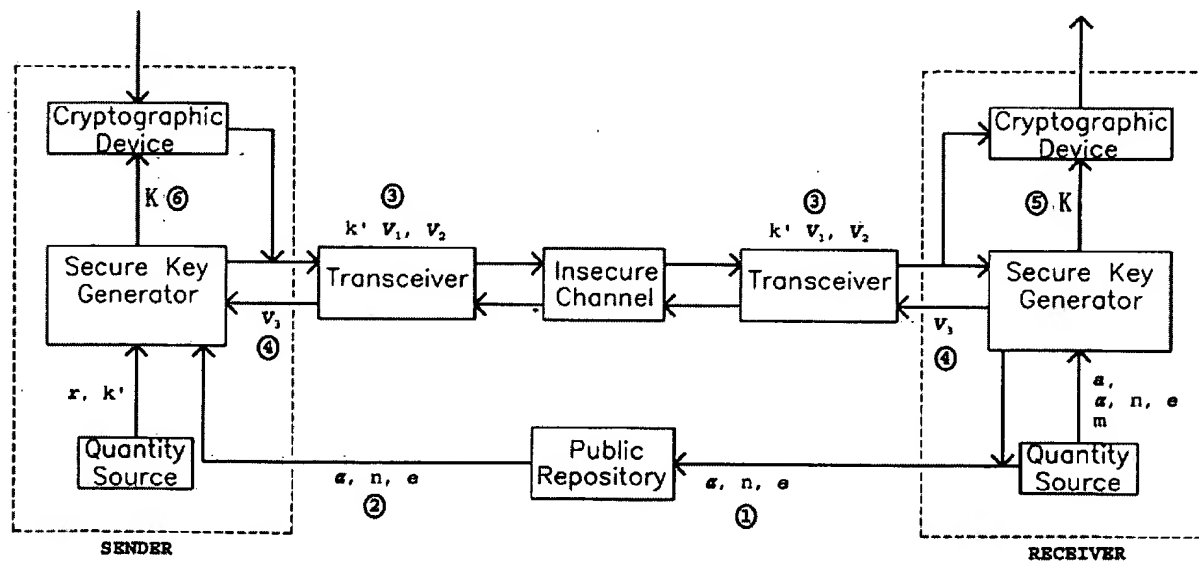
<sup>3</sup> Independent claim 1 element b.ii.  
Independent claim 14 element c.ii.(1)  
Independent claim 27 element a.ii.(1)

<sup>4</sup> Independent claim 1 element c.i.  
Independent claim 14 element c.i.(2) (a)  
Independent claim 27 element a.i.(2) (a)

<sup>5</sup> Independent claim 1 element c.ii.  
Independent claim 14 element c.i.(2) (b)  
Independent claim 27 element a.i.(2) (b)

6. The sending unit S uses at least some of the plurality of public quantities and the receiver's quantity in computing the key K.<sup>6</sup>

The following diagram, an annotated, redacted copy of the patent application's FIG. 1, graphically illustrates common characteristic elements 1-6 outlined above in the context of the patent application's detailed description.



<sup>6</sup> Independent claim 1 element d.  
Independent claim 14 element c.ii.(2)  
Independent claim 27 element a.ii.(2)

As illustrated above:

1. the receiver, enclosed within the dashed box at the right hand side of the preceding illustration, transmits for storage in the public repository the plurality of quantities  $\alpha$ ,  $n$  and  $e$  all of which are generated by the quantity source<sup>7</sup>;
2. the sender, enclosed within the dashed box at the left hand side of the preceding illustration, retrieves the plurality of quantities  $\alpha$ ,  $n$  and  $e$  from the public repository<sup>8</sup>;
3. the sender computes and transmits to the receiver three (3) quantities  $k'$ ,  $V_1$  and  $V_2$  using at least some of the plurality of quantities  $\alpha$ ,  $n$  and  $e$  retrieved from the public repository<sup>9</sup>;
4. the receiver computes and transmits to the sender a quantity  $V_3$  using at least some of the plurality of the public repository quantities  $\alpha$ ,  $n$  and  $e$ , and the quantities  $k'$ ,  $V_1$  and  $V_2$  received from the sender<sup>10</sup>;
5. the receiver computes the cryptographic key  $K$  using at least some of the plurality of public repository quantities  $\alpha$ ,  $n$  and

---

<sup>7</sup> See the pending application at page 17, line 4 through page 18, line 2.

<sup>8</sup> See the pending application at page 18, lines 20-23.

<sup>9</sup> See the pending application at page 18, line 23 through page 19, line 10.

<sup>10</sup> See the pending application at page 19, lines 11-19.



$e$ , and the quantities  $k'$ ,  $V_1$  and  $V_2$  received from the sender<sup>11</sup>;  
and

6. the sender computes the cryptographic key  $K$  using at least some of the plurality of public repository quantities  $a$ ,  $n$  and  $e$ , and the quantity  $V_3$  transmitted by the receiver<sup>12</sup>.

For authenticating a sender's digital signature, independent digital signature claim 40 requires the following steps performed by a receiving unit.

1. Retrieving a plurality of public quantities from a publicly accessible repository which the sending unit has previously stored there.
2. Using the digital signature, which the sending unit transmits together with message "M," and the plurality of public quantities, evaluating expressions of at least two (2) different verification relationships.
3. Comparing pairs of results obtained by evaluating the expressions of the at least two (2) different verification relationships.

---

<sup>11</sup> See the pending application at page 20, lines 1-6.

<sup>12</sup> See the pending application at page 20, lines 7-12.

Appl. No. 09/655,230  
Brief Dated August 29, 2005  
Appeal of

The Issues

1. Whether respective method, system and cryptographic unit claims 1-5, 12-18, 25-31, 38 and 39 are obvious under 35 U.S.C. § 103(a) based upon:
  - a. United States Patent no. 4,200,770 entitled "Cryptographic Apparatus and Method" that issued April 28, 1980, on a patent application filed by Martin E. Hellman, Bailey W. Diffie and Ralph C. Merkle ("the Hellman, et al. patent"); in view of
  - b. "Applied Cryptography" © 1996 by Bruce Schneier, published by John Wiley & Sons, Inc. ("Schneier").
2. Whether respective method, system and cryptographic unit claims 6-11, 19-24 and 32-37 are obvious under 35 U.S.C. § 103(a) based upon:
  - a. the Hellman, et al. patent; in view of
  - b. Schneier; and further in view of
  - c. United States Patent no. 5,159,632 entitled "Method and Apparatus for Public Key Exchange in a Cryptographic System" that issued October 27, 1992, on an application filed by Richard E. Crandall ("the Crandall '632 patent").
3. Whether digital signature claims 40 and 41 are anticipated under 35 U.S.C. § 102(b) by United States Patent no. 5,581,616 entitled "Method and Apparatus for Digital Signature Verifica-

Appl. No. 09/655,230  
Brief Dated August 29, 2005  
Appeal of

tion" that issued December 3, 1996, on a patent application filed by Richard E. Crandall ("the Crandall '616 patent").

#### Claim Group

Claims 1-39 rejections under 35 U.S.C. § 103(a) stand or fall by together.

Claims 40 and 41 rejections under 35 U.S.C. § 102(b) stand or fall by together.

#### Argument

On June 1, 2005, Applicant filed with the United States Patent and Trademark Office ("USPTO") a Response that presented arguments why claims 1-41 traverse the final rejections thereof appearing in the March 29, 2005, Office Action. On June 14, 2005, the USPTO issued an Advisory Action replying to the June 1, 2005, Response which maintained the final rejection of claims 1-41 appearing in the March 29, 2005, Office Action. The following arguments traverse the final rejection of claims appearing in the March 29, 2005, Office Action as those rejections are understood in light of the June 14, 2005, Advisory Action.

Appl. No. 09/655,230  
Brief Dated August 29, 2005  
Appeal of

**Cryptographic Key Establishing  
Claims 1-39 Are Patentable**

Independent cryptographic key establishing claims 1, 14 and 27 have been finally rejected as being obvious under 35 U.S.C. § 103(a) based upon:

1. the Hellman, et al. patent"); in view of
2. Schneier.

Some of dependent key establishing claims 2-13, 15-26 and 28-39 have also been finally rejected as being obvious under 35 U.S.C. § 103(a) based upon the Hellman, et al. patent in view of Schneier, while all of the remaining dependent claims have been rejected based upon the Hellman, et al. patent in view of Schneier and further in view of the Crandall '632 patent.

**Independent Claims 1, 14 and 27  
Are Patentable Over the Hellman,  
et al. Patent In View of Schneier**

In rejecting pending independent cryptographic key establishing claims 1, 14 and 27 as being obvious under 35 U.S.C. § 103(a), concerning the Hellman, et al. patent the June 14, 2005, Advisory Action on page 3 alleges as follows.

In reply to applicants argument that Hellman does not teach all the limitations of claim 27, specifically that the elements of a plurality of sender's quantities from the sending cryptographic unit and the at least some of the pluraltiy [sic] of public quantities are not taught, the values are in fact all disclosed: the public quantities q and a covers the at least some of the plurality of public quantites [sic] and the y1 covers the

Appl. No. 09/655,230  
Brief Dated August 29, 2005  
Appeal of

plurality of sender's quantities [sic] (Hellman, fig. 1 and col. 8:37-49; the variation using m-dimensional vector space defines a pluarlity [sic] of quantities for each of q, a and y1). (Emphasis supplied.)

Appellant first notes regarding the characteristics of the Hellman, et al. patent described in the June 14, 2005, Advisory Action that "the public quantities q and a" are generated and transmitted by the sending converser<sup>13</sup> rather than by the receiving converser<sup>14</sup>. The texts of independent key establishing claims 1, 14 and 27 all expressly require that only the receiving unit transmit for storage in a publicly accessible repository a plurality of public quantities.

Appellant respectfully submits that to the extent the June 14, 2005, Advisory Action maintains that q and a are included among the public quantities appearing in pending independent key establishing claims 1, 14 and 27, the text of the Hellman, et al. patent expressly contradicts the Advisory Action. Furthermore, the preceding misapplication of the Hellman, et al. patent in finally rejecting independent claims 1, 14 and 27, together with the other claims depending therefrom, demonstrates that the rejection of these claims relies upon either:

---

<sup>13</sup> See the Hellman, et al. patent's FIG. 1 and text in col. 3, line 1, and col. 4, lines 1-2 and line 7.

<sup>14</sup> See the Hellman, et al. patent's FIG. 1 and text in col. 3, lines 62-63.

1. an incorrect or fallacious reading of the text of the Hellman, et al. patent;
2. a deliberate, conscious avoidance of the Hellman, et al. patent's text; or
3. a deliberate, conscious avoidance of express limitations appearing in the texts of independent claims 1, 14 and 27, when the texts of those claims are construed in light of the patent application's specification.

**The Hellman, et al. Patent's Aptness  
To Independent Claims 1, 14 and 27**

Disclosures appearing in the Hellman, et al. patent, which are pertinent to the six (6) previously summarized shared characteristic elements of independent key establishing claims 1, 14 and 27, are summarized below.

1. A receiving converser 12<sup>15</sup> includes a key source 26 that generates a number/signal  $X_2$ <sup>16</sup>, i.e. an independent random number<sup>17</sup>. Receiving converser 12 keeps the number/signal  $X_2$  secret<sup>18</sup>. A secure key generator 22, included in receiving

---

<sup>15</sup> See the Hellman, et al. patent's FIG. 1 and text in col. 3, lines 62-63.

<sup>16</sup> See the Hellman, et al. patent's FIG. 1 and text in col. 4, line 8.

<sup>17</sup> See the Hellman, et al. patent in col. 4, lines 8-10.

<sup>18</sup> See the Hellman, et al. patent in col. 4, lines 13-14

converser 12, receives signals q and a, i.e. at least signal a is an independent random number<sup>19</sup>, from sending converser 11<sup>20</sup>. The secure key generator 22 of the receiving converser 12:

- a. generates  $Y_2$  by transforming with received signals q and a the receiving converser 12's secret  $X_2$ <sup>21</sup>; and
- b. transmits  $Y_2$  to the sending converser 11<sup>22</sup>.
2. A secure key generator 21 of the sending converser 11 receives  $Y_2$  from the receiving converser 12.<sup>23</sup>
3. The sending converser 11 uses  $Y_2$  only for generating its secure cryptographic key  $K$ ,<sup>24</sup> not for computing and transmitting to the receiving unit R a plurality of sender's quantities.
4. The receiving converser 12 uses signals q, a and  $Y_1$ <sup>25</sup>, all

---

<sup>19</sup> See the Hellman, et al. patent in col. 4, lines 8-10.

<sup>20</sup> See the Hellman, et al. patent in col. 4, lines 21-23.

<sup>21</sup> See the Hellman, et al. patent in col. 4, lines 23-27.

<sup>22</sup> See the Hellman, et al. patent in col. 4, lines 44-46.

<sup>23</sup> See the Hellman, et al. patent in col. 4, lines 44-46.

<sup>24</sup> See the Hellman, et al. patent in col. 4, lines 46-48.

<sup>25</sup> Note that, as described in col. 4 at lines 23-27, the secure key generator 21 of the sending converser 11 generates  $Y_1$  by transforming the sending converser's secret signal  $X_1$  with public signals q and a that are generated by the key source 25 included in the sending converser 11. Consequently, the sending converser 11

- received from the sending converser 11, only in generating its secure cryptographic key K,<sup>26</sup> not for computing and transmitting to the sending unit S at least one receiver's quantity.
5. The receiving converser 12 uses signals q, a and Y<sub>1</sub>,<sup>27</sup> all received from the sending converser 11, in generating its secure cryptographic key K.<sup>28</sup>
6. The sending converser 11 uses signals q, a and Y<sub>2</sub>, with only Y<sub>2</sub> being received from the receiving converser 12, in generating its secure cryptographic key K,<sup>29</sup>

There are many methods for implementing this form of the invention. The signals q and a may be public knowledge rather than generated by the key source 25. Further, it should be appreciated that the present invention has the capability of being modified by the use of additional transformations or exchanges of signals.

---

does not generate Y<sub>1</sub>, which the receiving converser 12 uses in establishing its cryptographic key K, using any sender quantity, no less a plurality of sender's quantities.

<sup>26</sup> See the Hellman, et al. patent in col. 4, lines 48-50.

<sup>27</sup> Note that, as described in col. 4 at lines 23-27, the secure key generator 21 of the sending converser 11 generates Y<sub>1</sub> by transforming the sending converser's secret signal X<sub>1</sub> with public signals q and a that are generated by the key source 25 included in the sending converser 11. Consequently, the sending converser 11 does not generate Y<sub>1</sub>, which the receiving converser 12 uses in establishing its cryptographic key K, using any sender quantity, no less a plurality of sender's quantities.

<sup>28</sup> See the Hellman, et al. patent in col. 4, lines 48-50.

<sup>29</sup> See the Hellman, et al. patent in col. 4, lines 48-50.



In some applications, it will prove valuable to have the  $i_{th}$  converser on the system generate  $Y_i$  as above and place it in a public file or directory rather than transmitting it to another converser with whom he wishes to communicate. Then two conversers  $i$  and  $j$  who wish to establish a secure channel will use  $K_{ij}=Y_i^{x_j} \bmod q=Y_j^{x_i} \bmod q$  as their key. The advantage is that converser  $i$ , having once proved his identity to the system through the use of his driver's license, fingerprint, etc., can prove his identity to converser  $j$  by his ability to compute  $K_{ij}$  and encrypt data with it.

Variations on the above described embodiment are possible. For example, in the above method based on logarithms modulo  $q$ ,  $m$ -dimensional vectors, each of whose components are between 0 and  $q-1$  could also be used. Then all operations are performed in the finite field with  $q^m$  elements, which operations are well described in the literature. (Col. 8, lines 20-43) Emphasis supplied.

Assume strictly for the sake of argument that the method disclosed in the Hellman, et al. patent:

1. were implemented using  $m$ -dimensional vectors, each of whose components are between 0 and  $q-1$ ;
2. that the  $m$ -dimensional vector signals  $q$  and  $a$ , generated by the sending converser 11, were made public knowledge; and
3. that the sending converser 11 and receiving converser 12 were to place their respective  $m$ -dimensional vector signals  $Y_1$  and  $Y_2$  in a public file or directory.

First, Appellant notes that under the preceding assumptions the Hellman, et al. patent's the receiving converser 12 places only a single quantity, i.e.  $m$ -dimensional vector signal  $Y_2$ , into a public file or directory. Considering characteristic elements 1. through 6. shared among independent key establishing claims 1, 14

Appl. No. 09/655,230  
Brief Dated August 29, 2005  
Appeal of

and 27, the Hellman, et al. patent could be interpreted so the m-dimensional vector signal  $Y_2$  is either:

1. a single public quantity placed in a publicly accessible repository as required by shared characteristic element 1.; or
2. one receiver's quantity transmitted to the sending converser 11 as required by shared characteristic element 4.

However, Appellant respectfully submits that properly interpreted the Hellman, et al. patent's m-dimensional vector signal  $Y_2$  cannot be both:

1. a single public quantity placed in a publicly accessible repository as required by shared characteristic element 1.; and
2. one receiver's quantity transmitted to the sending converser 11 as required by shared characteristic element 4.

Consequently, the Hellman, et al. patent must necessarily fail to disclose or to suggest either characteristic element 1., or characteristic element 4. shared among independent key establishing claims 1, 14 and 27.

Moreover, since characteristic element 6. shared among independent claims 1, 14 and 27 uses both:

1. the plurality of public quantities placed in a publicly accessible repository of shared characteristic element 1.; and
2. the receiver's quantity of shared characteristic element 4.;

Appl. No. 09/655,230  
Brief Dated August 29, 2005  
Appeal of

in establishing sender's key K, for the reasons set forth in the preceding paragraph the Hellman, et al. patent must necessarily fail to disclose or to suggest characteristic element 6.

In comparison with pending independent claims 1, 14 and 27, under the preceding assumptions the Hellman, et al. patent fails to disclose or to suggest any of characteristic elements 2., 3., 5. and 6., as well as either characteristic elements 1. or 4. that are shared among the independent key establishing claims 1, 14 and 27.

In making a comparison between the disclosure of the Hellman, et al. patent, when interpreted in accordance with the preceding assumptions, and pending claims 1, 14 and 27, it is noteworthy that two (2) of the public quantities  $\alpha$  and  $e$ , which the pending application discloses the receiving unit stores into the publicly accessible repository, are both linearly independent vectors<sup>30</sup>.

1. As demonstrated above, under a particular interpretation the Hellman, et al. patent fails to disclose or to suggest storing a plurality of public quantities into a publicly accessible repository of characteristic element 1. shared among independent key establishing claims 1, 14 and 27.
2. If one interprets the Hellman, et al. patent so the m-dimensional vector signal  $Y_2$  constitutes the public quantities which the receiving unit stores into the publicly

---

<sup>30</sup> See the present application on page 17, lines 17-20.

accessible repository, and if one interprets characteristic element 2. in light of the patent application's specification, then, because the specification discloses that the sending unit retrieves at least the quantities  $\alpha$ ,  $n$  and  $e$  from the public repository and because two (2) of the retrieved quantities  $\alpha$  and  $e$  are linearly independent vectors, the Hellman, et al. patent discloses that the sending converser 11 retrieves only the single  $m$ -dimensional vector signal  $Y_2$  from the publicly accessible repository, i.e. fails to disclose or to suggest characteristic element 2. shared among independent key establishing claims 1, 14 and 27.

3. While the sending converser 11 and receiving converser 12 are establishing their respective keys  $K$ , the sending converser 11 sends only the  $m$ -dimensional vector signals  $q$ ,  $a$  and  $Y_1$  to the receiving converser 12<sup>31</sup>. However, as disclosed in the Hellman, et al. patent in col. 4 line 7 and 23-27, the sending converser 11 generates the  $m$ -dimensional vector signals  $q$ ,  $a$  and  $Y_1$  entirely without retrieving any quantities from anywhere no than less from a publicly accessible repository. Consequently, the Hellman, et al. patent fails to disclose or to suggest computing a plurality of sender's quantities in

---

<sup>31</sup> See the Hellman, et al. patent's FIG. 1 and texts in col. 4 at lines 11-13 and 44-46.

accordance with the express requirements<sup>32</sup> of characteristic element 3. shared among independent key establishing claims 1, 14 and 27.

4. As demonstrated above, under a particular interpretation the Hellman, et al. patent fails to disclose or to suggest the receiver's quantity that is transmitted to the sending unit in characteristic element 4. that is shared among independent key establishing claims 1, 14 and 27.
5. Because the Hellman, et al. patent fails to disclose or to suggest the plurality of sender's quantities of characteristic element 3. shared among independent key establishing claims 1, 14 and 27, the Hellman, et al. patent necessarily fails to disclose or suggest the receiving unit using at least some of the plurality of sender's quantities in computing its cryptographic key K, i.e. fails to disclose or to suggest characteristic element 5. shared among independent key establishing claims 1, 14 and 27.
6. As demonstrated above, under either interpretation the Hellman, et al. patent fails to disclose or to suggest this characteristic element's computation of the sending unit's key

---

<sup>32</sup> Independent claims 1, 14 and 27 all require that the sending unit use at least some of the plurality of public quantities in computing the sender's quantities sent to the receiving unit.

Appl. No. 09/655,230  
Brief Dated August 29, 2005  
Appeal of

K of characteristic element 5. shared among independent key establishing claims 1, 14 and 27.

In rejecting pending independent cryptographic key establishing claims 1, 14 and 27 as being obvious under 35 U.S.C. § 103(a), concerning Schneier the June 14, 2005, Advisory Action on page 3 alleges as follows.

Finally, in reply to applicant's argument that Schneier adds nothing to the disclosure of Hellman et al., examiner disagrees since an explicit disclosure of a disinterested public repository and the role of the repository clearly teaches the limitation of a public repository for storing public quantities of the cryptographic system and further establishes several objectives as a set forth in Graham v. John Deere Co., 383 U.S. 1, 148 USPQ 459 (1966), specifically resolving the level of ordinary skill in the pertinent art and considering objective evidence present in the application indicating obviousness or nonobviousness. (Emphasis supplied.)

Appellant respectfully submits that Schneier's "explicit disclosure of a public repository" fails to fill gaps existing in the disclosure of the Hellman, et al. patent which, for the reasons explained in detail above, fails to disclose or to suggest any of characteristic elements 2., 3., 5. and 6., as well as either characteristic elements 1. or 4. that are shared among the independent key establishing claims 1, 14 and 27.

Appellant respectfully submits that for the reasons set forth in detail above, independent key establishing claims 1, 14 and 27, together with claims 2-13, 15-26 and 28-39 depending therefrom, when interpreted in the light of the pending patent application's

specification traverse rejection based upon the Hellman, et al.  
patent because that reference:

1. at best under one interpretation, expressly and implicitly discloses that its "receiver" stores only one quantity, m-dimensional vector signal "X<sub>2</sub>," into a publicly accessible repository;
2. at best under one interpretation, expressly and implicitly discloses that its "sender" retrieves only one quantity, m-dimensional vector signal "X<sub>2</sub>," from the publicly accessible repository;
3. fails to disclose or to suggest the "sender's" computing and transmitting to the "receiver" a plurality of sender's quantities using at least some of the plurality of public quantities;
4. at best under one interpretation, fails to disclose or to suggest that the "receiver" uses at least some of the plurality of public quantities and of the plurality of sender's quantities in computing and transmitting to the "sender" at least one "receiver's" quantity;
5. fails to disclose or to suggest that the "receiver" uses at least some of the plurality of public quantities and of the plurality of sender's quantities in computing its cryptographic key K; and

Appl. No. 09/655,230  
Brief Dated August 29, 2005  
Appeal of

6. fails to disclose or to suggest that the "sender" uses at least some of the plurality of public quantities and the receiver's quantity in computing its cryptographic key K.

For all of the preceding reasons independent cryptographic key establishing claims 1, 14 and 27 traverse rejection for obviousness under 35 U.S.C. § 103(a) based upon:

1. the Hellman, et al. patent"); in view of
2. Schneier.

Because claims 2-13, 15-26 and 28-39 respectively depend from independent cryptographic key establishing claims 1, 14 and 27, those claims also traverse rejection for obviousness under 35 U.S.C. § 103(a) based upon the Hellman, et al. patent in view of Schneier either alone or in combination with any other reference. For these reasons the Board of Appeal must overrule the rejections of cryptographic key establishing claims 1-39 appearing in the March 29, 2005, Examiner's Action, and find all of those claims to be patentable.

**Digital Signature Claims  
40 And 41 Are Patentable**

Independent digital signature claim 40 has been finally rejected under 35 U.S.C. § 102(b) as being anticipated by the Crandall '616 patent. Appellant respectfully submits that the



Appl. No. 09/655,230  
Brief Dated August 29, 2005  
Appeal of

final rejection of independent claim 40, together with claim 41 depending therefrom, relies upon either:

1. an incorrect or fallacious reading of the text of the Crandall '616 patent;
2. a deliberate, conscious avoidance of the Crandall '616 patent's text; or
3. a deliberate, conscious avoidance of express limitations appearing in the text of independent claim 40, when that claim's text is construed in light of the patent application's specification.

**The Crandall '616 Patent's Sender  
Stores Only One Quantity, ourPub,  
Into A Publicly Accessible Repository**

Regarding the disclosure of the Crandall '616 patent and the application of that reference to pending claims 40 and 41, as Appellant understands the March 29, 2005, Office Action's rejection of independent digital signature claim 40 in light of the June 14, 2005, Advisory Action, for reasons explained in greater detail below there can exist no rational dispute regarding the following facts.

1. The Crandall '616 patent expressly discloses that the "parameters are established for both sender and recipient" (receiver)<sup>33</sup>.
2. The Crandall '616 patent expressly discloses that:
  - a. the sender computes a public key ourPub<sup>34</sup>;
  - b. the receiver computes a public key theirPub<sup>35</sup>; and
  - c. the "two public keys ourPub and theirPub are published, and therefore known to all users"<sup>36</sup>.
3. The Crandall '616 patent lacks an express disclosure of who or what stores the parameters, in addition to theirPub and ourPub, used both by sender and recipient (receiver) into the public source 813.
4. The Crandall '616 patent expressly discloses that the sender and receiver retrieve parameters only from the public source 813.
5. That for a reference, e.g. the Crandall '616 patent, to anticipate a claim under 35 U.S.C. § 102(b), the reference

---

<sup>33</sup> See the Crandall '616 patent, col. 7, lines 23-32.

<sup>34</sup> See the Crandall '616 patent, col. 8 at lines 5-8.

<sup>35</sup> See the Crandall '616 patent, col. 8 at lines 9-13.

<sup>36</sup> See the Crandall '616 patent, col. 8 at lines 15-16.

Appl. No. 09/655,230  
Brief Dated August 29, 2005  
Appeal of

"must teach every aspect of the claimed invention either explicitly or impliedly."<sup>37</sup>

The preamble of independent claim 40 expressly requires that a sending unit "transmits for storage in a publicly accessible repository a plurality of public quantities." As described above, the body of independent claim 40 expressly requires that a receiving unit retrieve the plurality of public quantities from a publicly accessible repository which the sending unit has previously stored there.

Since irrefutably the Crandall '616 patent expressly discloses that the sender stores only ourPub into the publicly accessible repository, i.e. into the public source 813 appearing in that reference's FIGs. 8 and 12, independent digital signature claim 40 traverses rejection under 35 U.S.C. § 102(b) unless the sender must inherently, impliedly, store quantities in addition to ourPub into the publicly accessible repository which the receiver retrieves therefrom. For reasons explained in greater detail below, the sender disclosed in the Crandall '616 patent does not, as alleged in the March 29, 2005, Office Action, inherently, impliedly, store quantities in addition to ourPub into the publicly accessible repository.

---

<sup>37</sup> Manual of Patent Examining Procedure ("MPEP") Eighth Edition Revision 2, May 2004, § 706.02, p. 700-21

**Detailed Analysis Of The  
Crandall '616 Patent's Disclosures**

In rejecting pending independent claims 40 and 41 under 35 U.S.C. § 102(b) as being anticipated by the Crandall '616 patent, the March 29, 2005, Office Action on pages 3 and 4 alleges as follows.

7. Regarding the limitation of [1.] a sender storing a plurality of public quantities into the public source, which the receiver retrieves during digital signature authentication, figure 8 of Crandall identifies a public source (Reference No. 813) storing a plurality of public quantities for digital signature authentication. Crandall discloses the context of this public source as:

a separate source 813 stores publicly known information, such as the public keys "ourPub" and "theirPub" of sender 801 and receiver 802, the initial point (x1,y1), the field Fpk, and curve parameter "a". This source of information maybe a published directory, an on-line source for use by computer systems; or it may be transmitted [sic] between sender and receiver over a non-secure transmission medium. The public source 813 is shown symbolically connected to sender 801 through line 815 and to receiver 802 through line 814. [emphasis added] col. 12:63-13:4.

8. Hence, in the context of figure 8, the public keys, the initial point, the field, and the curve parameter are the plurality of public quantities stored (published), then used by the receiver to generate a mutual one-time pad to authenticate a digital signature signed by the sender. Crandall, 14:20-39. By virtue of the fact that the public source is defined only as a repository for public quantities, and the sender must share it's cryptographic context (sender's public key and context values (x1, y1), the Field Fpk, and curve parameter "a") with the receiver for proper generation of the one time pad, it is implicit in the disclosure that the plurality of public quantities is stored by the sender. This

Appl. No. 09/655,230  
Brief Dated August 29, 2005  
Appeal of

feature is further established in Figure 3, reference no. 303 and 16:4-9. (Emphasis supplied.)

FIGs. 8 and 12 of the Crandall '616 patent, which both depict the public source 813, fail to graphically illustrate storage of anything into the publicly accessible repository. That is, all arrows in FIGs. 8 and 12 point away from the public source 813.

Regarding reference no. 303 in FIG. 3, text in that block reads as follows.

PUBLISH, ourPub,  
theirPub,  
 $F_p$ ,  $k$ ,  $a$ ,  $(x_1, y_1)$

Clearly, the text appearing in FIG. 3, reference no. 303 doesn't identify who publishes the quantities  $F_p$ ,  $k$ ,  $a$ ,  $(x_1, y_1)$ .

Therefore, since FIGs. 3, 8 and 12 of the Crandall '616 patent all fail to disclose or to suggest who stores the initial point  $(x_1, y_1)$ , the field  $F_{pk}$ , and curve parameter "a" into the public source 813, the only place such disclosure might possibly occur is somewhere in the Crandall '616 patent's text.

The excerpt from the Crandall '616 patent beginning in col. 12 at line 63 and continuing to col. 13 line 4 appearing in the March 29, 2005, Office Action in the first sentence lists quantities that are stored in the public source 813. However, the cited text fails to disclose whether the plurality of public quantities are stored in the public source 813 by:

1. the sender;
2. the receiver; or

Appl. No. 09/655,230  
Brief Dated August 29, 2005  
Appeal of

3. a trusted third party.

Thus, the text excerpted in the March 29, 2005, Office Action fails to disclose or to suggest who stores the "publicly available parameters  $p$ ,  $F_{pk}$ ,  $(X_1/Z)$  and 'a'" into the public source 813.

Excerpted below is the text of the Crandall '616 patent's col. 16 at lines 4-9 which the March 29, 2005, Office Action cites in connection with FIG. 3, reference no. 303.

The present invention does not require that the private key be a prime number. Therefore, users can generate their own private keys, so long as a public key is generated and published using correct and publicly available parameters  $p$ ,  $F_{pk}$ ,  $(X_1/Z)$  and "a". (Emphasis supplied.)

Appellant observes that the Crandall '616 patent's text excerpted above also fails to disclose or to suggest who stores the "publicly available parameters  $p$ ,  $F_{pk}$ ,  $(X_1/Z)$  and 'a'" into the public source 813.

Regarding reference no. 303 in FIG. 3, the Crandall '616 patent's text in col. 8 at lines 14-16 expressly states only as follows.

Step 303

The two public keys ourPub and theirPub are published, and therefore known to all users. (Emphasis supplied.)

Thus, the Crandall '616 patent's text describing reference no. 303 in FIG. 3 also fails to disclose or to suggest who stores the "publicly available parameters  $p$ ,  $F_{pk}$ ,  $(X_1/Z)$  and 'a'" into the public source 813.

The preceding analysis of the Crandall '616 patent irrefutably establishes that the reference fails to expressly disclose, either in its FIGs. 3, 8 and 12 or in its texts, who stores the initial point  $(x_1, y_1)$ , the field  $F_{pk}$ , and curve parameter "a" into the public source 813.<sup>38</sup> Regarding the possibility that the Crandall '616 patent might, as alleged in the March 29, 2005, Office Action, "impliedly" disclose that the sender stores into the public source 813 at least one quantity in addition to ourPub, the text of the Crandall '616 patent in column 7 at lines 23-24 in a section of the reference entitled "Elliptic Curve Algebra" expressly states:

Next, parameters are established for both sender and recipient. (Emphasis supplied.)

The preceding excerpt from the Crandall '616 patent expressly discloses that parameters, e.g. the initial point  $(x_1, y_1)$ , the field  $F_{pk}$ , and curve parameter "a", are not established by either the receiver or the sender. Rather, the "parameters are established for both sender and recipient," apparently by some trusted third party.

Implicitly confirming the preceding interpretation of column 7's excerpt is the Crandall '616 patent's text in column 16 lines

---

<sup>38</sup> Pages 12-26 of the Response filed June 1, 2005, together with Exhibits A, B and C thereto present a comprehensive analysis of the Crandall '616 patent relevant to the public source 813 including FIGs. 8 and 12 thereof. Pages 12-26 of the Response filed June 1, 2005, together with Exhibits A, B and C thereto are hereby incorporated by reference as though set forth here.

1-4 which criticizes the RSA cryptosystem because a "user cannot generate its own private key in the RSA system." Contrasting the Crandall '616 patent's elliptic curve cryptosystem with the RSA cryptosystem is the Crandall '616 patent's text, excerpted above, that the March 29, 2005, Office Action cites in association with reference no. 3 in FIG. 3. Thus, the text of the Crandall '616 patent in column 16 lines 1-9 discloses that:

1. there exists cryptosystems which are so mathematically difficult, e.g. RSA, that a "user" cannot generate their own private key, no less generate their own public key;
2. for such difficult cryptosystems, a trusted third party must establish both the private and public keys; and
3. announces as a significant advance in cryptosystem technology the Crandall '616 patent's capability which permits a user to select their own private key.

If a user's ability to select their own private key constitutes a significant advance in cryptosystem technology warranting specific mention in the text of the Crandall '616 patent, wouldn't that reference be reasonably expected to similarly expressly announce in its text a sender's or receiver's ability to establish the elliptic curve cryptosystem's parameters such as the initial point  $(x_1, y_1)$ , the field  $F_{pk}$ , and curve parameter "a".

The only reasonable inference which can be drawn from the Crandall '616 patent's failure to specifically describe a user's



ability to establish cryptosystem's parameters such as the initial point  $(x_1, y_1)$ , the field  $F_{pk}$ , and curve parameter "a" is that establishing those parameters generally exceeds a user's capability due to the mathematical complexity and difficulty of the esoteric elliptic curve cryptosystem. Consequently, the text in column 16 impliedly confirms the statement excerpted from column 7 that the "parameters [stored in the public source 813 other than theirPub and ourPub] are established for both sender and recipient," probably by a highly mathematically-skilled, trusted third party.

For all of the preceding reasons, the entire Crandall '616 patent's disclosure fails to disclose or to suggest, either expressly or impliedly, that the sender stores anything other than ourPub into the public source 813. Rather, the text of the Crandall '616 patent expressly and impliedly discloses that:

1. the sender stores only a single quantity, i.e. ourPub, into the public source 813; and
2. other quantities, i.e. the cryptosystem's parameters, are stored into the public source 813 for both receiver and sender, apparently by a trusted third party.

Appl. No. 09/655,230  
Brief Dated August 29, 2005  
Appeal of

**Independent Claim 40's Text**  
**Distinguishes The Crandall '616 Patent**

As described above, the body of independent claim 40 further expressly requires that a receiving unit perform the following two (2) steps.

1. Using the digital signature, which the sending unit transmits together with message "M," and the plurality of public quantities retrieved from the publicly accessible repository, evaluating expressions of at least two (2) different verification relationships.
2. Comparing pairs of results obtained by evaluating the expressions of the at least two (2) different verification relationships.

In rejecting pending independent claims 40 and 41 under 35 U.S.C. § 102(b) as being anticipated by the Crandall '616 patent, the March 29, 2005, Office Action on page 4 alleges as follows.

9. Moreover, in figure 11, Crandall expressly teaches [2.] at least two expressions being evaluated by the receiver using a plurality of public quantities, [3.] and comparing the at least two expressions evaluated using a plurality of public quantities: reference no. 1105 identifies two expressions ( $e=x$  and  $f=x$ ) using a curve parameterized by public quantities "a", a field  $F_{pk}$  and initial point  $(X_1/1)$ , and the sender's public key; wherein only when  $e=x$  and  $f=x$  is the signature determined to be valid. Hence, Crandall teaches and/or suggests all limitations of claim 40. (Emphasis supplied.)

"FIG. 11 is a flow diagram illustrating the authentication of a digital signature . . . ." <sup>39</sup> Decision block reference no. 1105 in FIG. 11 of the Crandall '616 patent contains the following enigmatic text.

$$e, f = x$$

?

The text of the Crandall '616 patent describing reference no. 1105 in FIG. 11, which begins in col. 18 at line 61 and continues to col. 19 at line 4, states.

[a]t step 1104 the  $x$  values of  $P_1$  and  $P_2$  are used to determine values  $b$  and  $c$  and ultimately,  $e$  and  $f$ . This leads to to [sic] possible  $x$  values for the sum of  $P_1$  and  $P_2$ . At **decision block 1105** the argument " $e, f = x$ ?" is made to determine if either of the possible  $x$  values satisfies the equality of  $P_1 + P_2 = Q$ . If neither of the calculated  $x$  values satisfy the equation, that is, if the argument at decision block 1105 is false, the signature is not authentic and is indicated at block 1106. If one of the  $x$  values does satisfy the equation, that is, if the argument at decision block 1105 is true, a valid signature is assumed and indicated at block 1107. (Emphasis supplied.)

The preceding excerpt from the Crandall '616 patent clearly establishes that "a valid signature is assumed" if only "one of the  $x$  values" satisfies the equation. <sup>40</sup> Therefore, the preceding

---

<sup>39</sup> See the Crandall '616 patent in col. 18 at lines 48-49.

<sup>40</sup> The Crandall '616 patent, in a section entitled "DIGITAL SIGNATURE" which begins in col. 16 at line 9 and continues to col. 18 at line 26, describes the mathematical foundation for its digital signature authentication. That section of the Crandall '616 patent concludes with the following statements.

Appl. No. 09/655,230  
Brief Dated August 29, 2005  
Appeal of

excerpt from cols. 18 and 19 of the Crandall '616 patent expressly contradicts the allegation appearing on page 4 of the March 29, 2005, Office action excerpted above that "only when  $e=x$  and  $f=x$  is the signature determined to be valid."

Since as demonstrated in the immediately preceding paragraph the text of the Crandall '616 patent describing decision block 1105 expressly contradicts the March 29, 2005, Office Action's allegation, it is readily apparent that, as stated at the beginning of this section addressing the rejection of independent claim 40, the final rejection of that claim relies upon either:

1. an incorrect or fallacious reading of the text of the Crandall '616 patent; or
2. a deliberate, conscious avoidance of the Crandall '616 patent's text.

---

Therefore, the quadratic equation  $(x-e)(x-f)=0$  will generally have two solutions. One solution corresponds to an authentic signature. The other solution is extremely unlikely to have been selected at random, because the pool of  $x$  coordinates is of a size comparable to the elliptic curve. Therefore, when  $(x-e)(x-f)=0$  is satisfied, it can be safely assumed that the signature is authentic.

In practical application,  $P_1$  represents the calculated point  $P$  that is sent as part of the signature by the sender.  $P_2$  represents the expression  $M(\text{ciphertext}, P)^{\text{ourPub}}$ .  $Q$  of course represents  $u^0(X_1/1)$ .  $P_1+P_2$  represents  $R$  and is compared to  $Q$ .

Appl. No. 09/655,230  
Brief Dated August 29, 2005  
Appeal of

The text of steps 2 and 3 in independent claim 40 expressly encompasses the following operations.

b. using the digital signature and the plurality of public quantities, evaluating expressions of at least two (2) different verification relationships; and

c. comparing pairs of results obtained by evaluating the expressions of the at least two (2) different verification relationships.

The claims of a patent, which define the invention, are "to be construed in light of the specification and both are to be read with a view to ascertaining the invention." United States v. Adams, 383 U.S. 39, 49, 148 USPQ 479, 482 (1966). Indisputably,

[t]he meaning of every term used in any of the claims should be apparent from the descriptive portion of the specification with clear disclosure as to its import; and in mechanical cases, it should be identified in the descriptive portion of the specification by reference to the drawing, designating the part or parts therein to which the term applies. A term used in the claims may be given a special meaning in the description.<sup>41</sup>

It cannot be disputed that the present application on page 23 in lines 8-12 expressly states:

anyone receiving the plaintext message P to which the cryptographic unit 12b has appended the digital signature can verify the signature's authenticity by evaluating and comparing verification expressions set forth the two following pairs of verification relationships.

It cannot be disputed that the present application's description excerpted above gives a special meaning to the terms:

---

<sup>41</sup> Manual of Patent Examining Procedure ("MPEP") Eighth Edition Revision 2, May 2004, § 608.01(o), p. 600-81. See also Phillips v. AWH Corp. (Fed. Cir. 03-1269, -1286) (en banc) decided July 12, 2005.

Appl. No. 09/655,230  
 Brief Dated August 29, 2005  
 Appeal of

1. "expression;"
2. "pairs;" and
3. "verification relationships."

It cannot be disputed that the special meaning which the present application gives to the terms "expression," "pairs;" and "verification relationships" applies to the following two verification relationships appearing in the present application on page 23 in lines 13-16.

1. 
$$m^{((a.p)^n)(e \times (e \times a)) + a \times p} \cdot ((e \times a) + (e.a)^n e)$$

$$\frac{Q}{T} m^{-a \times (e \times a) \cdot p} m^{-a \times e (e.a)^n \cdot p}$$
2. 
$$m^{((a.p)^n)(e \times (e \times a)) + a \times p} \cdot ((e \cdot \alpha \times a)^n + (e \cdot \alpha \times a)(e \times a) \times (\alpha \times a) \times e)$$

$$\frac{Q}{T} m^{-((e \cdot \alpha \times a)^n + (e \cdot \alpha \times a)((e \times a) \times ((\alpha \times a) \times e) \times a \cdot p)}$$

It cannot be disputed that the Crandall '616 patent's digital signature, particularly in its text describing decision block reference no. 1150, fails to disclose or to even suggest "evaluating and comparing verification expressions set forth [in] two . . . pairs of verification relationships" as disclosed on page 23 of the pending application.

The authentication procedure disclosed in the Crandall '616 patent's decision block 1150 as described in that reference's text when applied to the verification relationships 1. and 2. disclosed in the present application on page 23 in lines 13-16 and excerpted above would necessarily require that:

1. the expressions appearing in both verification relationships on the right hand side of the  $\stackrel{?}{=}$  symbol be equal<sup>42</sup>, i.e. would necessarily require that

$$m^{-a \times (e \times a) : p} m^{-a \times e (e \cdot a)^n \cdot p} \\
= m^{-((e \cdot a \times a)^n + (e \cdot a \times a)((e \times a) \times ((a \times a) \times e) \times a \cdot p)},$$

which, based upon the present application's disclosure, is clearly fallacious; and

2. only one of the present application's verification relationships 1. and 2. would be satisfied in authenticating the digital signature<sup>43</sup>.

Consequently, in the terminology of independent claim 40 as that terminology must be construed in the light of the patent application's specification, the Crandall '616 patent fails to disclose or to suggest:

1. evaluating expressions of at least two (2) different verification relationships; and
2. comparing pairs of results obtained by evaluating the expressions of the at least two (2) different verification relationships.

---

<sup>42</sup> The same value "x" is compared both with e and f. See the Crandall '616 patent in col. 18, line 61 through col. 18, line 4.

<sup>43</sup> See the Crandall '616 patent in col. 18, line 61 through col. 18, line 4.

Appellant respectfully submits that for the reasons set forth in detail above, independent claim 40 together with claim 41 depending therefrom traverse rejection based upon the Crandall '616 patent because:

1. the Crandall '616 patent expressly and implicitly discloses that its "sender" stores only one quantity, "ourPub," into a publicly accessible repository; and
2. the Crandall '616 patent fails to disclose or to suggest:
  - a. evaluating expressions of at least two (2) different verification relationships; and
  - b. comparing pairs of results obtained by evaluating the expressions of the at least two (2) different verification relationships.

For the preceding reasons, the Board of Appeal must overrule the rejections of claims 40 and 41 appearing in the March 29, 2005, Examiner's Action, and find those claims to be patentable.

#### Conclusion

For reasons explained in detail above, independent cryptographic key establishing claims 1, 14 and 27, together with claims 2-13, 15-26 and 28-39 respectively depending therefrom, traverse rejection for obviousness under 35 U.S.C. § 103(a) based upon the Hellman, et al. patent in view of Schneier either alone or in combination with any other reference.

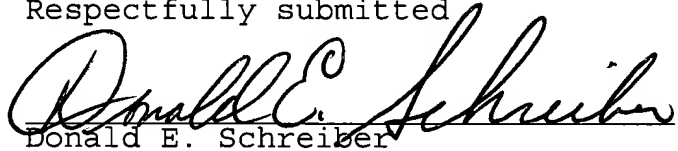


Appl. No. 09/655,230  
Brief Dated August 29, 2005  
Appeal of

Similarly, for reasons explained in detail above, independent digital signature claims 40, together with claim 41 depending therefrom, traverse rejection under 35 U.S.C. § 102(b) as being anticipated by the Crandall '616 patent.

For all the various reasons set forth above, the Board of Appeal must overrule the rejections of claims 1-41 appearing in the Examiner's Action dated March 29, 2005, and order that this application pass to issue.

Respectfully submitted



Donald E. Schreiber  
Reg. No. 29,435

Dated: 29 August, 2005

Donald E. Schreiber  
A Professional Corporation  
Post Office Box 2926  
Kings Beach, CA 96143-2926

Telephone: (530) 546-6041

Attorney for Appellant

Appl. No. 09/655,230  
Brief Dated August 29, 2005  
Appeal of



**APPENDIX I**  
**CLAIMS**

1. In a protocol for cryptographic communication via a communication channel "I" in which a sending cryptographic unit "S" transmits onto the communication channel I an encrypted cyphertext message "M" obtained by supplying both a plaintext message "P" and
- 5 a cryptographic key "K" to a first cryptographic device, and in which a receiving cryptographic unit "R" receives the cyphertext message M from the communication channel I and by supplying the cyphertext message M together with the key K to a second cryptographic device decrypts the plaintext message P therefrom, a method
- 10 by which the units S and R mutually establish a cryptographic key K by first exchanging messages before the sending unit S transmits the cyphertext message M comprising the steps of:
- a. the receiving unit R transmitting for storage in a publicly accessible repository a plurality of public

15 quantities;

  - b. the sending unit S:
    - i. retrieving the plurality of public quantities from the publicly accessible repository; and
    - ii. using at least some of the plurality of public

20 quantities, computing and transmitting to the receiving unit R a plurality of sender's quantities;

- c. the receiving unit R, using at least some of the plurality of public quantities and at least one of the plurality of sender's quantities received from the sending unit S:
  - i. computing and transmitting to the sending unit S at least one receiver's quantity; and
  - ii. computing the key K; and
- d. the sending unit S, using at least some of the plurality of public quantities and the receiver's quantity received from the receiving unit R, computing the key K.

2. The method of claim 1 wherein the receiving unit R, in storing the plurality of public quantities into the publicly accessible repository:

- i. selects a receiver's secret quantity;
- ii. selects for storage in the publicly accessible repository as part of the plurality of public quantities a plurality of selected public quantities; and
- iii. using the receiver's secret quantity and the plurality of selected public quantities, computes and stores in the publicly accessible repository as part of the plurality of public quantities a plurality of computed public quantities.

3. The method of claim 2 wherein the plurality of public quantities include a plurality of vectors.

4. The method of claim 2 wherein the plurality of selected public quantities include a plurality of vectors.

5. The method of claim 2 wherein the plurality of computed public quantities include a plurality of vectors.

6. The method of claim 2 wherein the sending unit S, in computing the plurality of sender's quantities for transmission to the receiving unit R:

- i. selects a sender's secret quantity;
- 5       ii. selects and transmits to the receiving unit R a one-time parameter; and
- 10       iii. using the sender's secret quantity, the one-time parameter and at least some of the retrieved plurality of public quantities, computes for transmission to the receiving unit R the plurality of sender's quantities.

7. The method of claim 6 wherein the plurality of sender's quantities include a plurality of vectors.

8. The method of claim 6 wherein the receiving unit R, in computing for transmission to the sending unit S the at least one receiver's quantity, uses the receiver's secret quantity, at least some of the plurality of public quantities, and at least one of the  
5 plurality of sender's quantities received from the sending unit S.

9. The method of claim 8 wherein the receiver's quantity includes at least one vector.

10. The method of claim 1 wherein the sending unit S, in computing the plurality of sender's quantities for transmission to the receiving unit R:

- i. selects a sender's secret quantity;
- 5 ii. selects and transmits to the receiving unit R a one-time parameter; and
- iii. using the sender's secret quantity, the one-time parameter and at least some of the retrieved plurality of public quantities, computes for transmission to the receiving unit R the plurality of  
10 sender's quantities.

11. The method of claim 10 wherein the plurality of sender's quantities include a plurality of vectors.

12. The method of claim 1 wherein the receiving unit R, in computing for transmission to the sending unit S the at least one receiver's quantity, uses a receiver's secret quantity, at least some of the plurality of public quantities, and at least one of the  
5 plurality of sender's quantities received from the sending unit S.

13. The method of claim 12 wherein the receiver's quantity includes at least one vector.

14. A system adapted for communicating as an encrypted cyphertext message M a plaintext message P that has been encoded using a cryptographic key K, the system comprising:

- a. a communication channel I adapted for transmitting the  
5 cyphertext message M;
- b. a pair of transceivers that are coupled to said communication channel I, and that are adapted for communicating the cyphertext message M from one transceiver to the other transceiver via said communication channel I; and
- 10 c. a pair of cryptographic units each of which is respectively coupled to one of said transceivers for transmitting the cyphertext message M thereto or receiving the cyphertext message M therefrom, each cryptographic unit:
  - i. when the cryptographic unit is to receive the  
15 cyphertext message M:

(1) storing plurality of public quantities in a publicly accessible repository;

20 (2) receiving via the communication channel I a plurality of sender's quantities from a sending cryptographic unit, and using the plurality of sender's quantities and at least some of the plurality of public quantities in computing:

25 (a) at least one receiver's quantity which said receiving cryptographic unit transmits via the communication channel I to said sending cryptographic unit; and

(b) the key K; and

30 ii. when the cryptographic unit is to send the cyphertext message M, retrieving the plurality of public quantities from the publicly accessible repository and using them in computing:

35 (1) the plurality of sender's quantities which the sending cryptographic unit transmits via the communication channel I to the receiving cryptographic unit; and

(2) after receiving via the communication channel I the receiver's quantity from the receiving cryptographic unit, the key K; and

- 40                   iii. including a cryptographic device having:
- (1) a key input port for receiving the key K from  
the cryptographic unit;
  - (2) a plaintext port:
    - 45                   (a) for accepting the plaintext message P for  
encryption into the cyphertext message M  
that is transmitted from the cryptograph-  
ic device, and
    - (b) for delivering the plaintext message P  
obtained by decrypting the cyphertext  
50                   message M received by the cryptographic  
device; and
  - (3) a cyphertext port that is coupled to one of  
said transceivers:
    - 55                   (a) for transmitting the cyphertext message M  
to such transceiver, and
    - (b) for receiving the cyphertext message M  
from such transceiver.

15. The system of claim 14 wherein said cryptographic unit  
which receives the cyphertext message M in storing the plurality of  
public quantities into the publicly accessible repository:

- (a) selects a receiver's secret quantity;



- 5                   (b) selects for storage in the publicly accessible repository as part of the plurality of public quantities a plurality of selected public quantities; and
- 10                   (c) using the receiver's secret quantity and the plurality of selected public quantities, computes and stores in the publicly accessible repository as part of the plurality of public quantities a plurality of computed public quantities.

16. The system of claim 15 wherein the plurality of public quantities include a plurality of vectors.

17. The system of claim 15 wherein the plurality of selected public quantities include a plurality of vectors.

18. The system of claim 15 wherein the plurality of computed public quantities include a plurality of vectors.

19. The system of claim 15 wherein the sending cryptographic unit, in computing the plurality of sender's quantities for transmission to the receiving cryptographic unit:

- i. selects a sender's secret quantity;

- 5           ii. selects and transmits to the receiving cryptographic  
            ic unit a one-time parameter; and
- iii. using the sender's secret quantity, the one-time  
            parameter and at least some of the retrieved plu-  
            rality of public quantities, computes for transmis-  
10           sion to the receiving cryptographic unit the plu-  
            rality of sender's quantities.

20. The system of claim 19 wherein the plurality of sender's quantities include a plurality of vectors.

21. The system of claim 19 wherein the receiving cryptographic unit, in computing for transmission to the sending cryptographic unit the at least one receiver's quantity, uses the receiver's secret quantity, at least some of the plurality of public quantities,  
5   ties, and at least one of the plurality of sender's quantities received from the sending cryptographic unit.

22. The system of claim 21 wherein the receiver's quantity includes at least one vector.

23. The system of claim 14 wherein the sending cryptographic unit, in computing the plurality of sender's quantities for transmission to the receiving cryptographic unit:

- i. selects a sender's secret quantity;
- 5 ii. selects and transmits to the receiving cryptographic unit a one-time parameter; and
- 10 iii. using the sender's secret quantity, the one-time parameter and at least some of the retrieved plurality of public quantities, computes for transmission to the receiving cryptographic unit the plurality of sender's quantities.

24. The system of claim 23 wherein the plurality of sender's quantities include a plurality of vectors.

25. The system of claim 14 wherein the receiving cryptographic unit, in computing for transmission to the sending cryptographic unit the at least one receiver's quantity, uses a receiver's secret quantity, at least some of the plurality of public quantities, and  
5 at least one of the plurality of sender's quantities received from the sending cryptographic unit.

26. The system of claim 25 wherein the receiver's quantity includes at least one vector.

27. A cryptographic unit adapted for inclusion in a system for communicating as an encrypted cyphertext message M a plaintext

message P that has been encoded using a cryptographic key K, the system including:

- 5           a. a communication channel I adapted for transmitting the cyphertext message M; and
- b. a pair of transceivers that are coupled to said communication channel I, and that are adapted for communicating the cyphertext message M from one transceiver to the
- 10           other transceiver via said communication channel I;

the cryptographic unit being adapted for coupling to said transceivers for transmitting the cyphertext message M thereto or receiving the cyphertext message M therefrom, and comprising:

- a. ports:
  - 15           i. when the cryptographic unit is to receive the cyphertext message M, for:
    - (1) storing plurality of public quantities in a publicly accessible repository;
    - (2) receiving via the communication channel I a
    - 20           plurality of sender's quantities from a sending cryptographic unit, and the receiving cryptographic unit using the plurality of sender's quantities and at least some of the plurality of public quantities in computing:
    - 25           (a) at least one receiver's quantity which said receiving cryptographic unit trans-

mits via the communication channel I to  
said sending cryptographic unit; and

(b) the key K; and

30           ii. when the cryptographic unit is to send the  
cyphertext message M, for retrieving the plurality  
of public quantities from the publicly accessible  
repository, the sending cryptographic unit using  
the retrieved plurality of public quantities in  
35           computing:

(1) the plurality of sender's quantities which the  
sending cryptographic unit transmits via the  
communication channel I to the receiving  
cryptographic unit; and

40           (2) after receiving via the communication channel  
I the receiver's quantity from the receiving  
cryptographic unit, the key K; and

b. a cryptographic device having:

45           i. a key input port for receiving the key K from the  
cryptographic unit;

ii. a plaintext port:

(1) for accepting the plaintext message P for  
encryption into the cyphertext message M that  
is transmitted from the cryptographic device,  
50           and

(2) for delivering the plaintext message P obtained by decrypting the cyphertext message M received by the cryptographic device; and

ii. a cyphertext port that is coupled to one of said transceivers:

(1) for transmitting the cyphertext message M to such transceiver, and

(2) for receiving the cyphertext message M from such transceiver.

28. The cryptographic unit of claim 27 wherein, when receiving the cyphertext message M, in storing the plurality of public quantities into the publicly accessible repository:

(a) selects a receiver's secret quantity;

(b) selects for storage in the publicly accessible repository as part of the plurality of public quantities a plurality of selected public quantities; and

(c) using the receiver's secret quantity and the plurality of selected public quantities, computes for storage in the publicly accessible repository as part of the plurality of public quantities a plurality of computed public quantities.

29. The cryptographic unit of claim 28 wherein the plurality of public quantities include a plurality of vectors.

30. The cryptographic unit of claim 28 wherein the plurality of selected public quantities include a plurality of vectors.

31. The cryptographic unit of claim 28 wherein the plurality of computed public quantities include a plurality of vectors.

32. The cryptographic unit of claim 28, when sending the cyphertext message M, in computing the plurality of sender's quantities for transmission to the receiving cryptographic unit:

- i. selects a sender's secret quantity;
- 5       ii. selects and transmits to the receiving cryptographic unit a one-time parameter; and
- 10       iii. using the sender's secret quantity, the one-time parameter and at least some of the retrieved plurality of public quantities, computes for transmission to the receiving cryptographic unit the plurality of sender's quantities.

33. The cryptographic unit of claim 32 wherein the plurality of sender's quantities include a plurality of vectors.

34. The cryptographic unit of claim 32 wherein, when receiving the cyphertext message M, in computing for transmission to the sending cryptographic unit the at least one receiver's quantity, uses the receiver's secret quantity, at least some of the plurality of public quantities, and at least one of the plurality of sender's quantities received from the sending cryptographic unit.

35. The cryptographic unit of claim 34 wherein the receiver's quantity includes at least one vector.

36. The cryptographic unit of claim 27 wherein, when sending the cyphertext message M, in computing the plurality of sender's quantities for transmission to the receiving cryptographic unit:

- i. selects a sender's secret quantity;
- ii. selects and transmits to the receiving cryptographic unit a one-time parameter; and
- iii. using the sender's secret quantity, the one-time parameter and at least some of the retrieved plurality of public quantities, computes for transmission to the receiving cryptographic unit the plurality of sender's quantities.



37. The cryptographic unit of claim 36 wherein the plurality of sender's quantities include a plurality of vectors.

38. The cryptographic unit of claim 27 wherein, when receiving the cyphertext message M, in computing for transmission to the sending cryptographic unit the at least one receiver's quantity, uses a receiver's secret quantity, at least some of the  
5 plurality of public quantities, and at least one of the plurality of sender's quantities received from the sending cryptographic unit.

39. The cryptographic unit of claim 38 wherein the receiver's quantity includes at least one vector.

40. In a protocol for communication in which a sending unit S transmits onto the communication channel I a message "M" together with a digital signature, and, wherein before transmitting the message M and the digital signature, the sending unit S transmits  
5 for storage in a publicly accessible repository a plurality of public quantities, a method by which a receiving unit R that receives the message M and the digital signature verifies the authenticity of digital signature comprising the steps performed by the receiving unit R of:

Appl. No. 09/655,230  
Brief Dated August 29, 2005  
Appeal of

- 10        a.    retrieving the plurality of public quantities from the  
publicly accessible repository;
- b.    using the digital signature and the plurality of public  
quantities, evaluating expressions of at least two (2) different  
verification relationships; and
- 15        c.    comparing pairs of results obtained by evaluating the  
expressions of the at least two (2) different verification  
relationships.

41. The method of claim 40 wherein the plurality of public  
quantities include a plurality of vectors.